Testimony of Linton F. Brooks
Under Secretary for Nuclear Security and
Administrator, National Nuclear Security Administration
Committee on Energy and Commerce,
Subcommittee on Oversight and Investigations
Hearing on NNSA Security
March 18, 2005

INTRODUCTION

Mr. Chairman, members of the Committee, thank you for this opportunity to address security at the National Nuclear Security Administration' s nuclear weapons research and production facilities. I would like to cover three major areas:

- **NNSA's progress on improving physical security**
- **NNSA's progress on improving the security of classified material**
- **NNSA's progress on improving Federal supervision of contractor security operations.**

It is important to recognize that there are other important security areas such as material control and accounting, the management of personal security clearances and human reliability, counterintelligence, and cyber security. Mr. Podonsky and I would be happy to respond to questions in these areas but because they have not been contentious I will not cover them in my statement.

Let me begin by stating none of the vital national security assets entrusted to the NNSA--nuclear weapons, Special Nuclear Material, or classified materials-- are at risk anywhere within the nuclear weapons complex. Our security program is robust and effective. Secretary Bodman has re-affirmed the Department's commitment to the security of the nuclear weapons complex.

At the same time, there have been significant security problems at some of our sites. Later in this statement I will describe what we have been doing to correct those problems and where we still have work to do.

PHYSICAL SECURITY

In the past three and one half years, physical security at NNSA sites has been dominated by the need to respond to the increased threat in the aftermath of the attacks of September 11, 2001. Prior to 2001 we assumed a relatively limited threat of attackers who sought to steal a weapon. For example, we could counter the threat by trapping the attackers in a weapons vault so they could not escape. 9/11 taught us that larger attacks were possible and that terrorists were willing to die to inflict massive damage. We shifted to a strategy of denying the attacker any access to nuclear weapons. In May 2003, based on an Interagency Working Group postulated threat, the Secretary approved a Design Basis Threat (DBT)that significantly increased the number of attackers against which we plan. Because the May 2003 DBT dramatically increased both the numbers and sophistication of the adversaries, it will take until the end of Fiscal Year 2006 for the Department to be fully compliant. That effort is on track within NNSA and all our facilities will meet the requirements of the May 2003 Design Basis Threat by the end of FY2006.

In May, 2004 the Department undertook a review of all available threat intelligence. Mr. Podonsky and I will be happy to discuss the results of that review in detail in closed session. As a result of that review, the former Deputy Secretary approved changes to our graded protection strategy for certain types of special nuclear materials and a further increase in the size of the attack against which we

must defend. His decision was codified in an October 2004 revision of the Design Basis Threat. Once again, we will be happy to go into details in closed session. The revised threat sets an exceptionally demanding standard and uses very conservative planning assumptions. We plan to meet this new standard by the end of FY2008.

A new round of vulnerability assessments is under way across the complex to determine enhancements required to meet this threat. Sites will submit their implementation plans and resource requirements by the end of July 2005. Once these plans have been reviewed, we will be able to formulate the impact of these requirements on security costs, but almost certainly additional resources will be required in FY2007 beyond those shown in our budget projections.

Many will conclude that such an attack is highly unlikely. No matter how low the probability, however, the potential consequences demand that we deter our enemies and deny them access to nuclear weapons or special nuclear materials.

To deal with this threat we have increased the number of uniformed protective forces, added barriers, closed roads, increased security patrols and detection procedures, increased access controls, and enhanced employee awareness of potential threat concerns. We were forced by necessity to meet the increase in threat with proven near-term solutions that rely on the application of more guards and guns—costly measures that we cannot afford to apply indefinitely.

Because of this we are also focusing on consolidation of special nuclear

material and on increased use of technology. At the Y-12 plant, one of our oldest sites, we are implementing a modernization strategy to consolidate special nuclear material storage and operations in facilities with designed denial features. Non-SNM operations will be moved outside high security areas to reduce costs. Construction of the Highly Enriched Uranium Materials Facility, which will provide us with more secure storage for SNM, has begun and is scheduled for completion in April 2008. In the interim, the site has provided for additional delay through an innovative use of large containers to form de facto forts protecting areas of greatest concern.

At Los Alamos National Laboratory, we have removed critical special nuclear materials from five facilities since 2001 and consolidated those operations within a single technical area. Material from Los Alamos' Technical Area 18 is currently being moved to the Device Assembly Facility on the Nevada Test Site— a facility designed for high levels of security in a more defendable area. Prior to the recent Los Alamos stand down, we expected TA-18 to be empty by September of this year. (Some of the material scheduled to go to Nevada will be stored on an interim basis within the protected area of the plutonium production facility.) We are still evaluating whether this schedule can be met without compromising safety. Any delay will be brief.

At Sandia National Laboratories in New Mexico, shut down of the Sandia Pulsed Reactor in 2007 will end operations with special nuclear material at that site. Over the longer term, I have charged the Weapons Complex Review Team to look into ending all plutonium operations at Lawrence Livermore National Laboratory in California, while still maintaining Livermore's capability to participate in the Stockpile Stewardship program. This team is examining the future of the entire weapons complex and will present its findings in late April.

NNSA has also begun to work with the Department's Office of Nuclear Energy, Office of Science and the Office of Environmental Management to evaluate the use of two facilities at the Idaho National Laboratories for interim storage of material from throughout the NNSA complex. One of these facilities was built to provide high levels of security for reprocessing of spent nuclear fuels; the other is a well-protected material storage building. We are in the opening stages of this evaluation and still must determine any legal barriers and additional physical security or construction requirements, but these facilities may offer exceptional opportunity to consolidate materials and components in a location with robust security features in place.

Consolidation is important, but it alone is insufficient for protecting nuclear materials from terrorists. America's strength is in technology. To continue the transformation of security in the nuclear weapons complex we must harness the technological prowess of the United States to reduce our reliance on manpower-intensive solutions. We have already begun deployment of advanced concept armored vehicles and remotely operated weapons systems at Y-12. We are

beginning integration of smart camera systems into the existing security systems at two facilities. Y-12 will also be implementing new vehicle detection and assessment systems and a new access delay system that utilizes activated delay technology that will not damage facilities.

In the longer term, we are looking at employment of additional active denial systems, remotely operated weapons, and more advanced detection systems that will reduce our reliance on manpower and provide earlier detection and attrition of an adversary. The Nevada Test Site will serve as a test platform for developing these concepts. To ensure the effective use of technology and system design we have established a Safeguards and Security Engineering Team with representatives from each of our sites and several of our Federal components to share best practices for physical security and to conduct peer reviews of proposed new security line item construction projects. This Team has already completed reviews of projects at Los Alamos and Y-12. Finally, we are working with Mr. Podonsky's Office of Safety and Security Performance Assurance to expedite the fielding of technology developed in the past but not fully implemented.

While consolidation and technology help, security will always depend on well-trained protective forces. While most of our protective forces are dedicated and competent, we have had problems. Three years ago, for example, the Sandia protective force had significant problems with officers sleeping on duty, incidents of racial tension and a general unprofessional attitude. Under our direction, Sandia took major steps to improve the leadership and supervision of the force. To ensure those steps are adequate, I commissioned a retired Air Force Major General to

assist my local Site Office in overseeing corrective action. Based on both my personal observation and on those of my subordinates, I believe the performance and morale of the Sandia protective force is vastly improved.

Starting two years ago we had significant problems with lost keys at both the Y-12 plant and the Lawrence Livermore National Laboratory. Although in no case could these keys allow access to special nuclear material or classified information, we saw their loss as a sign that security procedures needed improvement. In addition to instituting improved procedures, we concluded we had too many keys. I therefore established an initiative to move to a "keyless" environment. At Y-12, for example, we have reduced the number of security keys by 85 percent and no key type security locks are used to protect special nuclear materials.

Working with Mr. Podonsky's Office of Safety and Security Performance Assurance, we are working toward creation of a true elite para-military force at all our sites. Progress is steady, though uneven. For example, an independent assessment by Mr. Podonsky's office last summer uncovered sub-standard performance by the protective force (and other contractor elements) at the Nevada Test Site. The NNSA Site Manager turned over the routine operation of the federal Nevada Site Office to her Deputy and took personal supervision of the recovery plan. While corrective action is well along, I am disturbed by what this incident says about the quality of NNSA's day-to-day supervision of our contractors. I will have more to say on this point in a few minutes.

<u>CLASSIFIED MATERIAL CONTROL</u>

Security of nuclear materials must be matched by security of classified information. To improve our ability to protect such information, we have initiated efforts to reduce classified holdings at all facilities by destroying excess classified material and moving some holdings to areas where they can be better controlled. At Y-12, for example, we have moved over 1 million pounds of classified materials to approved long-term storage containers. Similar efforts are underway at all facilities.

The Committee is well aware of the problems with classified removable electronic media (CREM) at Los Alamos National Laboratory. In July 2004 the Laboratory Director imposed a stand down on essentially all activities because of a series of safety and security problems, including an inability to locate two classified computer disks. While separate investigations by the University of California, NNSA, and the FBI all concluded that the missing disks never existed, they also revealed serious problems with security management at Los Alamos. I would like to provide the Committee for the record a copy of the report prepared by the former Deputy Secretary of Energy and myself that outlines the problems in detail. I would also like to submit for the record a copy of a letter outlining the significant reduction in the management fee awarded the University of California for the operation of Los Alamos that I imposed as a result of these deficiencies. In addition, the Laboratory took disciplinary action including terminating three individuals, demoting several supervisors and suspending several individuals without pay.

In addition to correcting the specific performance problems at Los Alamos, the Department has tightened restrictions on accountable CREM. We now require

that these items be maintained in centralized lending libraries with formal checkout procedures enforced by full time trained custodians. Still, a contributing cause of the problem at Los Alamos was that we simply have too much classified material throughout NNSA and the rest of DOE. Los Alamos itself, for example, has gone from over 90,000 pieces of accountable CREM in January, 2004 to about 23,000 in September. To reduce this number further, we need to move to a diskless workstation computing environment. When classified information is stored on central servers with no desktop ability to remove such information, we will be able to significantly reduce the potential for inadvertent or intentional mishandling of classified information. We are now forming a task force under my supervision to accelerate the shift to diskless computing throughout the entire Department.

One element of both physical security and classified material control is control of access. We are conducting analysis of the current access control infrastructure throughout the nuclear weapons complex and examining technologies used by the private industry. This analysis will establish a baseline for enhancements to ARGUS, an access control and intrusion detection system that has become the standard application for NNSA facilities. We have also formed an Integrated Project Team for dealing with Homeland Security Presidential Directive 12 - Policy for a Common Identification Standard for Federal Employees and Contractors, which requires "smart cards" for physical and logical access to Federal sites, buildings and systems.

FEDERAL SUPERVISION

I would like now to turn to Federal supervision of security. Congress created NNSA in response to security lapses at our national security laboratories. While I believe we have had a number of successes in various areas, I am aware that this Committee and Congress as a whole will judge us by the degree to which we ensure adequate security throughout the weapons complex.

Shortly after assuming my current position, I became concerned that I did not have adequate competent security professionals to carry out my responsibilities. In the short term, I sought to deal with this problem by additional recruiting, but to ensure the long-term health of the Federal security community, in March 2003 I commissioned retired Admiral Hank Chiles to conduct an extensive review. Such a review had not been conducted previously. As a result, we are implementing a Human Capital Management Program to revitalize the Federal security work force that oversees security at our laboratories, plants, and storage facilities. In addition to provisions for the formal training and certification of Federal security officials, we will soon implement an intern program designed to attract and train the new Federal security officers who will provide leadership and guidance to the NNSA of the future.

To provide further focus and clear direction, in June, 2004 I created a new Associate Administrator for Defense Nuclear Security, reporting directly to me on an equal footing with the heads of my major programs. This office consolidated all NNSA security functions and is headed by a security professional with over 35 years of security experience both at Headquarters and in the field, as well as recent

experience in the Nuclear Regulatory Commission's Office of Nuclear Security and Incident Response.

Under the NNSA structure I have established, supervision of contractors in all areas—security, safety, and business practices—is carried out by Federal Site Offices located at each of the eight NNSA facilities. Last summer, when investigation of the apparently missing disks at Los Alamos began to reveal significant security management problems, I became concerned not just by the problems themselves but by the fact that they came as a surprise to the security professionals at the Site Office. This was in marked contrast to the safety problems at Los Alamos, all of which we were aware of in advance.

My concern heightened when the contractor at Nevada performed poorly on a periodic inspection by Mr. Podonsky. I was not as concerned with the actual performance—if no one ever does poorly the tests are too easy—as with the fact that the Site Office expected much better performance. As a result of these two incidents I personally led a team of senior security officials to the six sites with special nuclear material. At each site I focused on security performance and, in particular, on how supervision of the contractor was conducted. The results varied widely. At some sites we had impressive supervision, with strong involvement of the Site Manager, an active program of surveillance and inspection, and an exceptional understanding of the strengths and weaknesses of the contractor performance. At other sites we were far poorer.

Following my review, I concluded that I needed improvements in four areas: leadership failures, inadequate numbers of trained Federal security experts, a lack of hands-on involvement, and failure to provide sufficient headquarters supervision. We took the following actions to correct these problems:

- **Not surprisingly, the most important determinant of our effectiveness was the leadership provided by the senior security professional at each site. After consulting with the local federal Site Manager, I replaced two of the six senior security officials (I had previously replaced one other). A second leadership issue involved the local Site Managers themselves. Although they were the senior Federal official at each site, some had a tendency to leave supervision of security to their subordinates. I have corrected this.**

- **As a result of the Chiles Commission I referred to earlier, we were already working on improving training and qualification of our security professionals. In addition, we are just finishing a detailed review of staffing that will result in increases in the numbers of security professionals at most Site offices.**

- **A third problem concerned our method of supervising the contractor. In the area of safety our experts spend a great deal of time out in the facility observing operations. At the better sites, this is true for security as well, but at some sites our security experts spent much of their time reviewing paper rather than conducting hands on observations, except for an annual survey conducted over a period of less than a month. We are gradually shifting our approach to emphasize continuous surveillance as a supplement to annual surveys.**

- **Finally, my only check on the performance of the Site Offices was the inspections conducted every other year by the Office of Security and Safety Performance Assurance. To provide assistance to Site Managers and assurance to me that our performance is adequate in between these inspections, I am moving to formally establish an Office of Performance Assurance under the Associate Administrator for Defense Nuclear Security. The Office will assess and validate security performance across the NNSA and identify opportunities for improvement. It will work closely with the Office of Security and Safety Performance Assurance in the conduct and response to annual security surveys and periodic independent oversight reviews. I am confident that this new Office will strengthen the capabilities of individual site offices to perform effective supervision of NNSA's security contractors.**

In parallel with this effort, initially at my request and subsequently at the request of another Committee of Congress, the Office of Security and Performance Assessment conducted a review of NNSA supervision of security. Their conclusions validated my own and also indicated the need for greater attention to monitoring of corrective actions. I believe we have provided the Committee a copy of that review. I believe the steps we have put in place will dramatically improve our supervision of security at our sites.

CONCLUSION

NNSA remains fully committed to maintaining the security of the national treasures we guard. I am as confident of the security of our facilities as at any time in my tenure. I am not, however, satisfied. It is essential that we continue the security improvements we have underway, upgrade the protective forces, and improve Federal supervision. Only by doing so can we discharge our responsibilities, fix our problems as they occur, and ensure the long-term security of the nuclear weapons complex.

Thank you for your attention. I look forward to your questions.